

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

FILED

OCT 28 2020

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

In the Matter of the Search of)
THE PREMISES LOCATED AT: The residence of 11474 Pike 12,)
Frankford, Missouri, 63441 within the Eastern District of Missouri, a)
Single-Family residence with two (2) detached storage units.)
(See Attachment A.))

4:20 MJ 5243 NAB

FILED UNDER SEAL

SIGNED AND SUBMITTED TO THE COURT FOR FILING
BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Ryan Brown, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the Eastern District of Missouri, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

Title Section
18 2252 and 2252A

distribution and receiving child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.



Applicant's signature

Ryan Brown, TFO, FBI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: October 28, 2020



Judge's signature

City and State: St. Louis, Missouri

Honorable Nannette A. Baker, U.S. Magistrate Judge

Printed name and title

AUSA: JILLIAN ANDERSON

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT: The)
residence of 11474 Pike 12, Frankford,)
Missouri, 63441 within the Eastern District of)
Missouri.)

No. 4:20 MJ 5243 NAB

FILED UNDER SEAL

)
SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

AFFIDAVIT

I, Ryan Brown, being duly sworn, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 11474 Pike 12, Frankford, Missouri, 63441 (hereinafter the “Premises”) further described in Attachment A, for the things described in Attachment B. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code, Sections 2252 and/or 2252A have been committed by Robert Bliss or other persons known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

2. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation’s (“FBI”) Child Exploitation Task Force. I have been a Task Force Officer for four (4) months and have been a sworn Police Officer with the St. Charles County, Missouri Police Department for approximately five (5) years. I am also assigned as an investigator to the Missouri Internet Crimes Against Children Task Force. I have conducted numerous investigations regarding the sexual

exploitation of children that involve the use of a computer which has been used to commit a crime in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. As a Task Force Officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information. I have experience utilizing computers during my career as an investigator and I have completed multiple in-service training, outside training, and other courses in computer crime investigation.

3. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Sections 2252 and 2252A, which criminalize, among other things, the production, possession and/or receipt and distribution of child pornography, and other related materials. The items that are the subject of the search and seizure applied for in this affidavit are more specifically described in Attachment A.

4. The statements contained in this affidavit are based on my personal knowledge or information provided to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2252, and 2252A including, but not limited to, the items described in Attachment A, which is attached hereto and incorporated by reference, will

be found within the property to be searched.

LOCATION TO BE SEARCHED

5. The location to be searched is the Premises, further described as:

11474 Pike 12, Frankford, MO 63441 is a single-family residence. The residence sits on the west side of Pike 12, also known as “County Road 12” and is located between Hwy MM and Hwy C. The residence has red and tan in color brick and brown shingle roofing. There are three windows on the front (east side) of the residence and the window are surrounded by dark in color shutters. “11474” is posted in gold numerics on the front of a gray in color mailbox which is located at the end of the gravel/grass driveway. The front door of the residence is white in color and faces east. The front door also has an outer door (storm door) which is dark in color. An attached garage, which is white in color, is located on the south side of the residence.

Located in the back yard of the residence is a gray and white in color barn/storage area. The barn has a white in color tin style roof and an overhang on the east side. Underneath the overhang is appears to be a door/entryway into the barn.

Also located in the back yard on the north side of the property is another shed/storage area that is white in color that is positioned facing approximate south.

DEFINITIONS

6. The following terms have the indicated meaning in this affidavit.

7. “Digital device(s),” includes the following items and terms, and their respective definitions:

a. The term “computer” means an electronic, magnetic, optical, electrochemical, or

other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).

b. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including for example, tablets, digital music devices, portable electronic game systems, electronic game consoles and wireless telephones. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. "Wireless telephone or mobile telephone, or cellular telephone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic

“address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

d. “Digital storage media,” as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

e. A “tablet” is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touchscreen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, “wi-fi” networks, or otherwise. Tablets typically contain programs called applications (“apps”), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

f. A “GPS” navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated “GPS”) to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location and may contain records of the addresses or locations

involved in such historical navigation. that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

8. The term "minor" means any individual under the age of 18 years. 18 USC § 2256(1). Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person. 18 USC § 2256(2)(A).

9. Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).

10. Child pornography means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC § 2256(8)(A) or (C).

11. Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 USC § 2256(2)(A).

12. Identifiable minor means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).

13. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

14. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

15. The phrase "records, documents, and materials" as used herein, including those used to facilitate communications, includes all of the listed items of evidence in whatever form and by whatever means such records, documents, or materials may have been created or stored. Those forms and means of storage and creation include but are not limited to any handmade from (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, videotapes, motion pictures, photocopies); or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, and CD-ROMS), as well as printouts or readouts from any magnetic storage device.

16. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

17. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device, wireless telephones, or any other electronic mobile device).

18. IP Address: The Internet Protocol address (or simply "IP address") is a unique

numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

19. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

COMPUTERS AND CHILD PORNOGRAPHY

21. This affiant has participated in investigations of persons suspected of violating federal child pornography laws, including Title 18, United States Code, Sections 2251, 2252 and 2252A. I have also participated in various mandated and volunteer training for the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography.

22. Computers, computer hardware, wireless telephones, and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography was formerly produced using cameras and film (either still

photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of such items was most often accomplished through a combination of personal contacts, mailings, and telephone calls.

23. The development of computers, wireless telephones and computer hardware have changed the way in which individuals interested in child pornography interact with each other, as computers and computer hardware serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

24. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. Digital cameras and wireless telephones allow images to be transferred directly onto a computer. A device known as a modem permits computers to connect to other computers through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers and wireless telephones around the world.

25. The ability of computers, computer hardware and wireless telephones to store images in digital form makes them ideal repositories for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) has grown tremendously within the last several years. These drives can store hundreds of thousands of images at a very high resolution.

26. The Internet affords collectors of child pornography several different venues for

obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

27. Collectors and distributors of child pornography also utilize online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

28. As is the case with most digital technology, communications by way of computer, computer hardware and wireless telephones can be saved or stored on the devices. Storing this information can be intentional, i.e., by saving an e-mail as a file or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, Internet users generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains specific software, when the software was installed, logs regarding the usage of the software, and even some of the files which were uploaded or downloaded using the software. Such information may be maintained indefinitely until overwritten by other data.

29. A growing phenomenon on the Internet is peer to peer-file-sharing (hereinafter referred to as "P2P"). P2P file sharing is a method of communication available to Internet users

through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers. There are several different software applications that can be used to access these networks, but these applications operate in essentially the same manner.

30. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. Once the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's designated "shared" folder are available to anyone on the world wide network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the network. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. A user, however, is not required to share files in order to utilize the P2P network.

31. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user seeking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then selects the file(s) which he/she would like to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in an area previously designated by the user and will remain there until moved or deleted. The majority of the P2P software applications retain logs of each download event.

32. A person interested in sharing child pornography with others via a P2P network, needs only to place those files in his/her "shared" folder(s). Those files are then available to all users of the P2P network for download, regardless of their physical location.

33. A person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a search term, such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select a file(s) from the search results and the selected file(s) can be downloaded directly from the computer(s) sharing the file(s).

34. The computers that are linked together to form the P2P network are located throughout the world. Therefore, the P2P network operates in interstate and foreign commerce.

35. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel (i.e. the user can download more than one file at a time). In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this process is that it reduces the time it takes to obtain a file(s). A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. An IP address is expressed as four numbers separated by decimals. Each number, which can range from 0 to 256, is unique to a particular internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

36. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been

selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

37. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he/she often stores it in random order and with deceptive file names. The latter requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Moreover, the vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. As such, it is difficult to know prior to a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed,

password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

38. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files.

39. The BitTorrent network is a very popular and publically available P2P file sharing network. A peer/client computer can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others.

40. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other peer/clients on the network are able to download the files or pieces of files from them, a process which maximizes the download speed for all users on the network.

41. Files or sets of files are shared on the BitTorrent network via the use of “Torrents.” A Torrent is typically a small file that describes the file(s) to be shared. It is important to note that “Torrent” files do not contain the actual file(s) to be shared, but information about the file(s) to be

shared. This information includes the “info hash,” which is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent. This set of data contains the SHA-1 hash value of each file piece in the Torrent, the file size(s), and the file name(s). This “info hash” uniquely identifies the Torrent file on the BitTorrent network.

42. In order to locate Torrent files of interest and download the files that they describe, a typical user will use keyword searches on Torrent-indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent indexing websites do not actually host the content (files) described by Torrent files, only the Torrent files themselves. Once a Torrent file is located on the website that meets a user’s keyword search engine criteria, the user will download the Torrent file to their computer. The BitTorrent network client program on the user’s computer will then process that Torrent file to help facilitate finding other peer/clients on the network that have all or part of the file(s) referenced in the Torrent file.

43. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a Torrent-indexing website and conduct a key word search using a term such as “preteen sex” or “pthc” (pre-teen hardcore). Based on the results of the keyword search, the user would then select a Torrent of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the Torrent file. Utilizing BitTorrent network protocols, peer/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the Torrent file and that these file(s) are available for sharing. The user can then download the file(s) directly from the computer(s) sharing them. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file(s) with other users on the network. The downloaded file(s) are

then stored in an area or folder previously designated by on the user's computer or on an external storage media. The downloaded file(s), including the Torrent file, will remain in that location until moved or deleted by the user.

44. Law enforcement can search the BitTorrent network in order to locate individuals sharing child pornography images, which have been previously identified as such based on their SHA1 values. Law Enforcement uses BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file(s) is downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

45. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes (1) the suspect client's IP address; (2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and (3) the BitTorrent network client program and version being utilized by the suspect computer. Law enforcement can then log this information.

46. The investigations of P2P file sharing networks in a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. The ICAC Task Force Program uses law

enforcement tools to track IP addresses suspected (based on SHA1 values and file names) of trading child pornography. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of whom were also involved in contact sexual offenses against child victims.

47. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

48. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

49. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

50. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other

paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. "Child Erotica" includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

51. Child pornography collectors may reinforce their fantasies by taking progressive, overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

52. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, such as their vehicle(s),

where it is readily available. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

53. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, some collectors rarely dispose of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

SEARCH METHODOLOGY TO BE EMPLOYED

54. The search procedure of electronic data contained in computer, wireless telephones, computer hardware, computer software, and/or memory storage devices may include the following techniques (NOTE: The following is a non-exclusive list, as other search procedures may be employed):

a. Examination of all of the data contained in such computers, computer hardware, wireless telephones, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as listed in Attachment A;

b. Searching for and attempting to recover any deleted, hidden, and/or encrypted data

to determine whether that data falls within the list of items to be seized as listed in Attachment A (any data that is encrypted and/or unreadable will be returned when law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

- c. Surveying various file directories and the individual files they contain;
- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

PROBABLE CAUSE & DETAILS OF INVESTIGATION

55. On January 26th, 2020, members of the St. Charles County Cyber Crimes Task Force, the Missouri Internet Crimes Against Children Task Force (MOICAC) and the FBI Child Exploitation Task Force initiated a child pornography investigation.

56. This affiant has had numerous contacts and dealings with informants, other law enforcement officials, subjects known to possess and trade obscene material, and subjects known to possess images of child pornography. This affiant has attended courses related to child pornography and computer technology including, but not limited to, Internet Crimes Against Children Investigative Techniques, and Internet Undercover Operations.

57. Law enforcement officers in MOICAC are familiar in the use of software programs that enable law enforcement officers to conduct searches to identify users on the BitTorrent network in the state of Missouri that have been documented as advertising, and/or offering to share child pornography files, at least in part, with other users on the BitTorrent network.

58. This affiant knows from training and experience and/or from other law enforcement officers in MOICAC, a Secure Hash Algorithm Version 1 (or SHA1) is essentially the fingerprint of a photograph or video- a digital signature- and no two (2) are alike. If there are two (2) copies of the same picture/video, when the SHA1 values of the pictures/videos are compared, the SHA1 values will match. In fact, based on information from the National Institute of Standards and Technology one can conclude that two (2) files are identical with a precision that greatly exceeds 99.9 percent certainty. The use of SHA1 values is so reliable that information concerning SHA1 values is gathered by various nationwide law enforcement agencies to locate computers distributing in part, images believed to be child pornography.

59. This affiant knows from training and experience and/or from other law enforcement officers in MOICAC that Internet computers identify each other by an Internet Protocol or IP address. This Affiant knows that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead a law enforcement officer to a particular Internet service company and that company can typically identify the account that uses or used the address to access the Internet.

60. During an authorized internet undercover operations on January 26th, 2020, Detectives with MOICAC identified a computer that was offering to participate in the distribution of child pornography using the BitTorrent Peer-to-Peer file sharing network. The Internet Protocol

(IP) address of the computer sharing the computer files was 107.191.207.174. Using a peer-to-peer file sharing software, set to download from a single source, this affiant was advised by other law enforcement officer in MOICAC the download was able to download multiple computer files from the computer. Those files contained suspected child pornography. Specifically, those files contained videos of minor children engaged in sexually explicit conduct. Detectives copied those files to a computer disk.

61. On Sunday, January 26th, 2020, between 2233 hours and 2246 hours, detectives with MOICAC successfully completed the download, through the BitTorrent program, of the following file(s) that the device at IP address 107.191.207.174 was making available, because it was associated with a torrent with the infohash: dceecff5d2891eed7b18bb0eef585fb3290c7120. This torrent file references one (1) file, of which was identified as being a file of investigative interest to child pornography investigations.

62. The device at IP address 107.191.207.174 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address. The downloaded file is described as:

File Name: [JulyJailbait]- Fuck my girl like adult pthc.mp4

SHA1: 2LH5PNZ2A6WYOHABJK2VMKMEUDQJL43V

Description: This video file is an .mp4 file. The video is approximately 18 minutes and 19 seconds in length. The video begins with a prepubescent female laying on her back on what appears to be a bed and the female is masturbating. The female is completely nude, wearing only a pink mask to partially cover her face. After approximately 14 seconds of the female masturbating, an adult male subject enters the video and is kneeling on the bed. The adult male is nude from the

waist down and is only wearing a t-shirt and a mask to cover his face. The female continues with the female performing oral sex on the male subject as she is still laying on her back and masturbating. The video continues with the prepubescent female and adult male subject engaging in sexual intercourse in various positions until the adult male ejaculates inside of the female's vagina. The female is described as prepubescent due to her overall diminutive stature and lack of anatomical growth.

63. On Sunday, January 26th, 2020, between 2042 and 2104 hours, detectives with MOICAC successfully completed the download, through the BitTorrent program, of the following file(s) that the device at IP address 107.191.207.174 was making available, because it was associated with the torrent with the infohash:

120941d770e2d9f84d21cfdac3763e5bb155370. This torrent file references one (1) file, of which was identified as being a file of investigative interest to child pornography investigations.

64. The device at IP address 107.191.207.174 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address. The downloaded file is described as:

File Name: Julyjailbait - children's reactions to child porn compilation pthc preteen MK.mp4

SHA1: 4N2YRQVZNXT2GXIOBJIIHYWP77ID6L2

Description: This video is approximately 00:09:29 long. The video depicts what appears to be young, adolescent females reacting to multiple videos and photographs of child pornography. The following is a further description of some of the individual clips and pictures within the entire video:

- At 00:00:10 a prepubescent female is seen performing oral sex on an erect penis.
- At 00:00:54 a prepubescent female is shown sitting on top of an adult male while his erect penis is penetrating her vagina.
- At 00:04:15 a prepubescent female is seen being bent over on a bed or couch while an adult male penetrates her vagina with his erect penis. In the top left corner of the video there is text labeling the prepubescent female as a six year old by the name of Rona.
- At 00:06:45 a prepubescent female is lying on her back while an adult male is penetrating her vagina with his erect penis.
- At 00:09:13 a prepubescent female is being bent over a table while an adult male is penetrating her vagina from behind. The female is wearing a black colored dress and black heels. In the top left corner of the video there is text labeling the prepubescent female as a nine year old by the name of Judy-An.

The females are described as prepubescent due to their overall diminutive stature and lack of anatomical growth.

65. On February 8th, 2020, an investigative computer running Roundup eMule Version 1.63, was successful in locating and downloading one (1) file of interest related to child pornography. The software is a Peer 2 Peer file sharing software which allows for the single source downloading of files believed or known to be child pornography. The investigative computer directed the investigative focus to a device at IP address 107.191.207.174. This detailed log for the Peer to Peer program on the suspect device also revealed the username from the suspect device as “**Blisszilla**”. The one file observed is:

538F583D19873B781D9F36E6410E4527.

66. On February 8th, 2020 between 12:36:02 hrs. and 12:36:28 hrs., the investigative computer successfully completed the download of the one (1) file that the device at IP address 107.191.207.174 was making available. The device at IP Address 107.191.207.174 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address. The video is described as follows:

Ed2k Hash: 538F583D19873B781D9F36E6410E4527

SHA1: 6HU4TUSIOD6HEIJIQFP7IM3K5OU5GOC4

Description: This is a video which is approximately 5 minutes and 18 seconds in length. The video depicts a prepubescent white female that is fully clothed. At approximately 1 minute and 20 seconds, the female begins to remove her pants and expose her genitals to the camera. At approximately 2 minutes in the video the female spreads her legs and uses her hands to further spread her genitals open for the camera. The female is described as prepubescent due to her overall diminutive stature and lack of anatomical growth.

67. On February 12th, 2020, detectives with MOICAC conducted a query on the IP address 107.191.207.174 through the geolocation website, maxmind. Maxmind reported the IP address 107.191.207.174 to be registered to Ralls Technologies, LLC.

68. On February 12th, 2020, This Affiant requested an investigative subpoena be sent to Ralls Technologies, LLC. for information on the above IP address for the dates and times reported.

69. On February 20th, 2020 Detectives with MOICAC conducted an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated for a device at IP address 107.191.207.174, because it was associated with a torrent

with the infohash: 29e766a7994da35b75eed63e5c82e17a1a1244c0. This torrent file references 1 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP address 107.191.207.174, also referred to as the “suspect device”. The Suspect Device reported it was using BitTorrent client software -SZ27:2- Shareaza 2.7.10.2.

70. On February 20th, 2020, between 1933 hrs and 2046 hrs, Detectives with MOICAC observed a partial download was successfully completed of the following 1 file that the device at IP address 107.191.207.174 was making available:. The device at IP Address 107.191.207.174 was the sole candidate for each download, and as such, each files was downloaded directly from this IP Address. The file is described as follows:

Filename: Lolitashouse - Secret Area 34 - 10Yr, 11Yr, & 12Yr Blds Strip & Play on Bed.avi

Sha1: WTYJNEJGACWPNAG7N24GGNCLFSZQYSS6

Description: This is a video which is approximately 14 minutes 48 seconds in length. It starts off with three young females who appear to be in the early stages of puberty due to their overall small stature, childlike face, and slight breast development. The females take off each other cloths and lay on a bed like item. At 1:25 in the video the girls start lightly touching each other’s genitals which are clearly displayed for the camera. At approximately 9:00 in the video one of the female straddles another female so they can perform oral sex on each other.

71. On March 3rd, 2020 an investigative computer running Roundup eMule Version 1.63, was successful in locating and downloading one (1) file of interest related to child

pornography. The software is a Peer 2 Peer file sharing software which allows for the single source downloading of files believed or known to be child pornography. The investigative computer directed the investigative focus to a device at IP address 107.191.207.174, because it was associated with one file which is known or a suspected file of child pornography. The one file observed is: FF14901624E4136E08C0A4E978B3D082.

72. On March 3rd, 2020 between 21:52:29 hrs. and 22:36:28 hrs., the investigative computer successfully completed the download of the 1 file that the device at IP address 107.191.207.174 was making available. The device at IP Address 107.191.207.174 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address. The file is described as follows:

Ed2k Hash: FF14901624E4136E08C0A4E978B3D082

SHA1: 3RZ7664GCUJI6H4GEI45KSEGH5F45NOY7

Description: This is a video which is approximately 5 minutes 23 seconds in length. The video starts with a prepubescent female dancing around in a pink shirt, a pink skirt, and white underwear. At approximately 0:45 in the video the female takes off her underwear and displays her genitals for the camera. The female uses her hands to further display her genitals and at approximately 1:30 inserts a finger in to her vagina. At 2:00 the female obtains a green sexual aid and inserts it in to her vagina and masturbates. At approximately 3:05, the female removes the sexual aid from her vagina and inserts it in to her anus. The video has the female masturbating with the sexual aid until approximately 4:47. At this time, the video jumps to another scene of what appears to be the same female in different clothing masturbating with the same sexual aid.

The female appears to be prepubescent due to overall diminutive stature and lack of anatomical growth.

73. This Affiant observed each video file regarding this report and determined that each video file would be described as child pornography.

74. On March 5th, 2020, this Affiant received a response from Ralls Technologies, LLC regarding the investigative subpoena this Affiant submitted to the company for information on IP address 107.191.207.174 for the dates and times of 01/26/2020 at 22:30:20 CST and 02/08/2020 at 12:36:04 CST. Ralls Technologies provided the following subscriber information:

Name: Robert Bliss
Address: 11474 Pike 12, Frankford, MO 63441-2522

75. A search of the residence through an online law enforcement database called idicore system news returned with the following possible residents of 11474 Pike 12, Frankford, MO 63441:

Bliss, Robert
XX/XX/1974
XXX-XX-4100

Bliss, Crystal N.
XX/XX/1983
XXX-XX-6133

76. On Friday, March 6th, 2020 this Affiant along with another member of MOICAC conducted surveillance at the residence described above as 11474 Pike 12, Frankford, MO 63441, a single-family residence. The residence sits on the west side of Pike 12, also known as “County Road 12” and is located between Hwy MM and Hwy C. The residence has red and tan in color brick and brown shingle roofing. There are three windows on the front (east side) of the residence

and the window are surrounded by dark in color shutters. "11474" is posted in gold numerics on the front of a gray in color mailbox which is located at the end of the gravel/grass driveway. The front door of the residence is white in color and faces east. The front door also has an outer door (storm door) which is dark in color. An attached garage, which is white in color, is located on the south side of the residence.

Located in the back yard of the residence is a gray and white in color barn/storage area. The barn has a white in color tin style roof and an overhang on the east side. Underneath the overhang is appears to be a door/entryway into the barn.

Also located in the back yard on the north side of the property is another shed/storage area that is white in color that is positioned facing approximate south.

77. On March 6th, 2020 when this affiant drove past the above described residence, I observed a dark in color GMC Yukon SUV bearing Missouri license plates JA5-D2L. A search of that license plate through the Department of Revenue returned registered to Robert B. Bliss and Crystal N. Bliss at 11474 Pike 12, Frankford, MO 63441.

78. On July 9th, 2020, this affiant and another member of MOICAC conducted surveillance at the residence described above, 11474 Pike 12, Frankford, MO 63441. While driving past the residence, this affiant observed the dark in color GMC Yukon SUV, bearing Missouri license plates JA5-D2L, parked in the driveway of the residence. Another search of this license plate through the Department of Revenue returned registered to Robert B. Bliss and Crystal N. Bliss at 11474 Pike 12, Frankford, MO 63441.

79. On July 9th, 2020, while driving past the residence, this affiant also observed a dark in color Chevrolet Silverado Truck, bearing Missouri license plate 1HE-X02, parked in the

driveway of the residence next to the GMC Yukon described above. A search of this license plate through the Department of Revenue returned registered to Robert Bliss at 11474 Pike 12, Frankford, MO 63441.

80. On September 3rd, 2020, this affiant and another member of MOICAC drove past the residence 11474 Pike 12, Frankford, MO 63441. While driving past the residence, this affiant observed a dark in color Chevrolet Silverado truck that appeared to be the same Chevrolet truck that was registered to Robert Bliss, as described above.

81. On September 11th, 2020, this affiant and another member of MOICAC drove past the residence 11474 Pike 12, Frankford, MO 63441. Again, while driving past the residence, this affiant observed the same dark in color Chevrolet Silverado truck bearing Missouri license plate 1HE-X02, parked in the driveway of the residence. This truck is registered to Robert Bliss at the address listed above.

82. On October 13th, 2020, this affiant drove past the residence 11474 Pike 12, Frankford, MO 63441. Again, while driving past the residence, this affiant observed what appeared to be the same dark in color GMC Yukon, parked in front of the residence, parallel with the residence. Although a license plate was not observed on the GMC on this occasion, it appeared to be the same GMC Yukon that had been observed at the residence on previous occasions, which was registered to Robert and Crystal Bliss.

83. On October 21st, 2020, this affiant located documentation from the Pike County Sheriff's Office which revealed Robert Bliss had been charged with Child Molestation and Sexual Misconduct involving a subject less than 15 years of age from a report that was completed on March 28th, 2020. A review of the publicly available information on Missouri Case Net reveals

that Robert Bliss was arrested upon a warrant on or about August 19, 2020 with the address of Robert Bliss indicated on the warrant as the 11474 Pike 12, Frankford, MO 63441. He and was released on bond on or about September 22, 2020. This affiant also observed that Robert Bliss had been served with a full order of protection, prohibiting him from having contact with an unnamed juvenile.

84. On October 21st, 2020, this affiant contacted the Pike County Prosecutor's Office and was advised that a condition of Robert Bliss' release on bond with GPS monitoring and was that he was not to be at the residence of 11474 Pike 12, Frankford, MO 63441, where the victim in the Pike County case resides. It is believed that Robert Bliss is, for the duration of the bond condition, temporarily residing with a family member in Louisiana, MO. As per this affiant's consultation with the private probation office overseeing the GPS monitoring of Robert Bliss, it is unclear where Robert Bliss is consistently staying during this temporary relocation. The Pike County Prosecutor's Office advised that the wife of Robert Bliss who is also the mother of the victim asked the Prosecutor's Office to dismiss the charges against Robert Bliss.

85. This affiant was provided with the report and supplemental reports regarding this investigation on October 22nd, 2020. Upon review of this documentation, this affiant observed the allegations of child molestation and sexual misconduct were from incidents that occurred between Robert Bliss and his step-daughter. This affiant observed the allegation was Robert Bliss would touch the juvenile's genitals, over her clothes, on different occasions as Robert Bliss would "play" with her.

86. This affiant also observed in the Pike County Sheriff's Office investigation that the juvenile victim disclosed during a forensic interview at the Child Advocacy Center in Hannibal,

MO, that Robert had asked her if she wanted to make \$30 by cleaning the house in a dress while not wearing any underwear.

87. This affiant also observed in the Pike County Sheriff's Office investigation that Robert Bliss' cell phone was seized for evidentiary purposes in order for a forensic examination to be completed due to statements made to the Pike County Sheriff's Office Sergeant that responded to the residence by Crystal Bliss. This affiant observed the statements made by in the report by Crystal Bliss were as follows:

"Crystal told me (the Pike County Sergeant) that she's suspected for a long time that Robert has a problem with viewing child pornography. I asked Crystal why she suspects Robert views child pornography. Crystal told me that in December of 2019, she obtained Robert's cellular phone and checked his web browser history. Crystal told me that upon reviewing his web history, she noticed Robert was searching for teenage female pornography. I asked Crystal if she would be willing to submit a voluntary statement form, she told me yes."

88. Upon observing the written statement completed by Crystal Bliss, this affiant observed Crystal Bliss stated the following in relation to child pornography:

"On previous events I found him looking up child porn and confronted him with that at which he said he has always had a porn problem/masturbation problem and needed help. He said he looked up child porn out of curiosity."

89. Furthermore, this affiant observed in the Pike County Sheriff's investigation that after the first forensic interview with the juvenile victim concluded, a short meeting occurred with Crystal Bliss, and the investigating officer, as well as a Division of Social Services investigator. It was reported that during this meeting that, when asked about the viewing of child pornography by

Robert Bliss, Crystal stated that while searching Robert's Google history on his cell phone she did not observe any images or videos of child pornography but she observed links or search terms for young teen models, step daughters, and "something else between the ages of 7-14."

90. Although Robert Bliss' cell phone was seized as part of the initial investigation, this affiant has knowledge from previous experience that people participating in the viewing and/or downloading of child pornography may use computers, tablets and other electronic devices as well as multiple electronic devices to conduct their searching and downloading of child pornography as well as storing child pornography.

IV. CONCLUSION

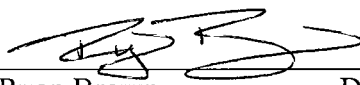
Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly possess, receive, and/or distribute child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment A of this Affidavit, are located within 11474 Pike 12, Frankford, MO 63441, and all computers, computer hardware, computer and digital media, and wireless telephones therein.

91. This Affiant requests authority to seize such material, specifically, that the Court issue a search warrant for the premises at 11474 Pike 12, Frankford, MO 63441 and the storage units on the property (listed above), and all computers, computer hardware, computer and digital media, and wireless telephones therein for the items listed in Attachment A.

92. In order to prevent the compromise of this on-going investigation, affiant respectfully requests that the application, affidavit and search warrant be sealed.


I state under the penalty of perjury that the foregoing is true and correct.

Respectfully submitted,



Ryan Brown Date 10/28/2020
Task Force Officer
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.



The Honorable NANNETTE A. BAKER Date 10/28/2020
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 11474 Pike 12, Frankford, MO 63441 (hereinafter the “SUBJECT PREMISES”) is a single-family residence. The residence sits on the west side of Pike 12, also known as “County Road 12” and is located between Hwy MM and Hwy C. The residence has red and tan in color brick and brown shingle roofing. There are three windows on the front (east side) of the residence and the window are surrounded by dark in color shutters. “11474” is posted in gold numerics on the front of a gray in color mailbox which is located at the end of the gravel/grass driveway. The front door of the residence is white in color and faces east. The front door also has an outer door (storm door) which is dark in color. An attached garage, which is white in color, is located on the south side of the residence.

Located in the back yard of the residence is a gray and white in color barn/storage area. The barn has a white in color tin style roof and an overhang on the east side. Underneath the overhang is appears to be a door/entryway into the barn.

Also located in the back yard on the north side of the property is another shed/storage area that is white in color that is positioned facing approximate south.

ATTACHMENT B

Property to be seized

All items which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing violations of 18 U.S.C. § § 2252 and 2252A, including but not limited to:

1. Any computer, digital device, cellular telephone, computer system, data processing devices, software, central processing units; internal and peripheral storage devices, fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, computer compact disks, CD-ROMS, DVDs, and other memory storage devices and related peripherals (hereinafter referred to collectively as Devices);
2. Peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and
3. Any devices, mechanisms or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).
4. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software or other programming code.
5. Any and all documents, data, records, emails, communications and internet history (in documentary or electronic form) pertaining to the possession, receipt, distribution or production

of child pornography and attempts thereof; any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and pertaining to an interest in child pornography or sexual exploitation of children.

6. Records, information, and items relating to the ownership or use of the Devices including sales receipts, bills for internet access, and handwritten notes.

7. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

8. Records, data and information relating to sexual exploitation of children, including correspondence and communications between users, traders and producers of child pornography and child exploitation material.

9. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.

10. Documents and records regarding the ownership, use and/or possession of the SUBJECT PREMISES.

11. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein

12. For any Devices, data, records and information whose seizure is otherwise authorized by this warrant:

a. evidence of who used, owned, or controlled the Devices, data, records and information at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing

history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the Devices were accessed or used to determine the chronological context of access, use, and events relating to the crime(s) under investigation and to the user of the Devices;

e. evidence indicating the user of the Devices knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the Devices;

h. evidence of the times the Devices were used;

i. passwords, encryption keys, and other access devices that may be necessary to access the Devices;

j. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices;

k. records of or information about Internet Protocol addresses used by the Devices;

l. records of or information about the Devices’s internet activity, including firewall

logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a search, review and analysis of electronic devices, electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the

investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.